AO 106 (Rev. 04/10) Application for a Search Warrant

SEALED

UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
computers that access the website "Hidden Service A" which is located at oqm66m6iyt6vxk7k.onion

Case No. 8:12MJ360

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*
See Attachment A, incorporated herein

located in the _____ District of Nebraska and elsewhere, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Sections 2251 and 2252A	Engaging in a Child Exploitation Enterprise, Conspiracy to Advertise, Receive and Distribute Child Pornography

The application is based on these facts:
See attached affidavit

United States District Court
District of Nebraska

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jeffrey Tarpinian
Applicant's signature

Jeffrey Tarpinian - Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/19/12

Judge's signature

City and state: OMAHA NE

F.A. Gossett U.S. Mag. Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

IN THE MATTER OF THE SEARCH OF COMPUTERS THAT ACCESS THE WEBSITE "HIDDEN SERVICE A"	)))	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Jeffrey Tarpinian, being first duly sworn, hereby depose and state:

A. INTRODUCTION AND AGENT BACKGROUND

1. I am presently employed as a Special Agent of the Federal Bureau of Investigation (FBI), and am assigned to the Cyber Crime Task Force of the Omaha Field Office in the District of Nebraska. I have been employed by the FBI since May of 1988, including four months of training at the FBI academy in Quantico, Virginia. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography, including violations pertaining to the production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. § 2252(a) and 2252A. My current duties include the full-time investigation of computer related crimes, and I have conducted over forty search warrants relating to crimes against children. As a result of my training and experience, I am familiar with information technology and its use in criminal activities. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of many state, local, and federal search warrants, a number of which involved child exploitation and/or child pornography offenses. I am an "investigative or law enforcement officer" of the United States within the meaning of Section

2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. I make this affidavit in support of an application for a search warrant to use a network investigative technique ("NIT") further described in this affidavit and its attachments.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies as described below; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/employees and U.S. Department of Justice computer forensic professionals; my experience, training and background as a Special Agent with the FBI, and communication with computer forensic professionals assisting with the design and implementation of the NIT. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

B. RELEVANT STATUTES

4. This investigation concerns alleged violations of: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. § 2252A(a)(5)(B), Knowing Access or Attempted Access With Intent to View Child Pornography.

a. 18 U.S.C. § 2252A(g) prohibits a person from engaging in a child exploitation enterprise. A person engages in a child exploitation enterprise if the person violates, inter alia, federal child pornography crimes listed in Title

18, Chapter 109A, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons;

b. 18 U.S.C. §§ 2251(d)(1) and (e) prohibits a person from knowingly conspiring to make, print or publish, or causing to be made, printed or published, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

c. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) prohibits a person from knowingly conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any

means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

C. DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

5. The following definitions apply to this Affidavit:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread" refers to a linked series of posts and reply messages. Message threads often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Bulletin Board Bdministrator.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A DNS (domain name system) server, in

essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written,

recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

k. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-

location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

m. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

n. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

p. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

q. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

D. PROBABLE CAUSE

The Tor Network

6. "Hidden Service A" operates on an anonymity network available to Internet users known as "The Onion Router" or "Tor" network. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.

7. The Tor software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's

actual IP address, shows up in the website's IP log. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor network operates similarly to a proxy server. Tor accordingly allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features, such as Torbutton and Torbrowser bundle. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

8. Tor also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services" operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from that website server.

Finding and Accessing "Hidden Service A"

9. As described below, law enforcement became aware of the location and contents of "Hidden Service A" upon the execution of search warrants at the home and office of Aaron McGrath, the administrator of "Hidden Service A." Because "Hidden Service A" is a Tor hidden

service, it cannot be accessed from the traditional Internet. Only a user who has installed Tor software on his/her computer may access the board. A user installs Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org. Even after connecting to the Tor network, however, a user must know the web address of "Hidden Service A" in order to access it. Rather than a plain language address like www.cnn.com, a Tor web address is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of "Hidden Service A" on Tor and obtain the web address for the board. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on "Hidden Service A" as well as its location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. "Hidden Service A" is listed in that section. Accessing "Hidden Service A" therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon "Hidden Service A" without understanding its purpose and content. Moreover, the name of "Hidden Service A" contains a direct reference to the sexual abuse of children. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses "Hidden Service A" has knowingly accessed with intent to view child pornography, or attempted to do so.

Seizure of "Hidden Service A"

10. On November 15, 2012, federal agents executed a search warrant at the home of

Aaron McGrath in Omaha, NE. McGrath had been connected to a child pornography bulletin board ("hereinafter CPBB") of which McGrath was the sole administrator.[1] McGrath was located in his bedroom typing on a laptop computer. Upon seeing agents, McGrath immediately closed the laptop computer, which locked the computer. Agents were able to determine the password and unlock the computer. Among other things, a web browser window was open and connected to CPBB. McGrath had been browsing a CPBB page titled "13 y/o girl pics," while logged in as the administrator of CPBB. Agents also noticed that the laptop computer was directly connected to the computer server with the IP address 208.88.77.241.

11. Also on November 15, 2012, law enforcement agents executed search warrants at Power DNN/Perigon Networks and Cosentry, web hosting companies in Bellevue, NE. There, agents located and copied the data on the computer server carrying IP address 208.88.77.241, which was labeled "Aaron." Forensic examination of that server confirmed that it was the computer server hosting CPBB. Also located on that computer server were two other Tor hidden services, "Hidden Service A" and "Hidden Service B." During the execution of the search warrants at the Power DNN/Perigon/Cosentry facility, agents located another computer server at that facility, which was labeled "Aaron 2." On November 17, 2012, agents accessed the server marked "Aaron 2." Upon

[1] That bulletin board is an active and operating child pornography bulletin board that has been operating since January of 2009 and is dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including methods and tactics of perpetrating child sex abuse and the safety and security of individuals who seek to sexually exploit children online. As of November 16, 2012, the board home page states that it has over 6,300 members, over 3,000 message threads, and over 24,000 postings. Among other things, it has an "Images" forum there are six subforums: "Babies," "Boys," "Girls," "JB Boys," "JB Girls," and "Misc." The "babies" subforum contains nearly 100 message threads, each of which message thread contains postings by board members, including images of child pornography depicting infant and toddler-aged children posed to expose their genitals or being subjected to sexually explicit conduct by adults. In total, it contains thousands of postings and messages containing child pornography images. Those images include depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children. Numerous of its users have made postings to the board stating that they were sexually abusing children and posting images depicting that sexual abuse.

review of that server, agents determined that server marked "Aaron" contained an old version of "Hidden Service A," whereas the server marked "Aaron 2" contained the current operating version of "Hidden Service A." The computer server marked "Aaron 2" was subsequently seized and moved to a government facility. At all times pertinent to this warrant, "Hidden Service A" will be operating at a government facility in Omaha, Nebraska the District of Nebraska.

Description of "Hidden Service A" and Its Content

12. On November 16 and 17, 2012, law enforcement agents accessed "Hidden Service A" via the Tor network and documented its contents. "Hidden Service A" is a Tor network social networking website dedicated to pedophilia and the advertisement and distribution of child pornography. The URL of "Hidden Service A" is "oqm66m6iyt6vxk7k.onion." The name of the site makes reference to pedophilia. The site lists over 7,000 members. The rules of the site, which are accessible on the main page to anyone who accesses "Hidden Service A," describe it as "a communication tool for fellow pedos to discuss their interests and share content" and that it is for "the discussion of our mutual pedophilic interests in a mature and civilized fashion." In my training and experience, "pedos" is a reference to pedophilia, and "content" refers to child pornography.

13. Users can register on "Hidden Service A" with a username and a password. Once registered, users can set up a profile that includes a picture, personal information, contact information, and other functions such as blogs, uploaded files, web pages, or polls. Many users have a user photo, sometimes called an "avatar," that is in and of itself child pornography. Although users can register and set up their own profile, most of the site is accessible to any user without registering or logging in. The only exceptions appear to be the pages of private groups and users' private messages, which are described below.

Child Pornography Images and Videos on "Hidden Service A"

14. One "Hidden Service A" section contains a "files" section that compiles all files posted by members. Within that section are images and videos. The section contains more than 17,000 images, all of which depict children. All of those images are accessible to any user who accesses the site. Those images depict minor children engaging in sexually explicit conduct with adults or other children, minor children posed while exposing their genitals, or images of child erotica. Most of those images are of prepubescent children. Many of those images depict infant and toddler-aged children being sexually abused by adults or posed to expose their genitals. There do not appear to be any adult pornographic images at all. The section also contains approximately 120 videos. The filenames are consistent with child pornography, including "Dad Cum in 4y0 mouth" and "smiling pretty 4y0 girl sucks big dick." Agents have reviewed videos posted which include videos of minor children, some of whom are prepubescent, engaging in sexually explicit conduct with adults or other children.

Groups on "Hidden Service A"

15. "Hidden Service A" also contains a groups section. There are approximately 330 groups as of November 17, 2012 (all group member numbers below are as of November 17, 2012). Any member may start a group. Within a group, members can post images and messages which are visible to all group members. Groups may be open or closed. There are approximately 59 closed groups – the rest are open. In an open group, all users who access the board, even those who have not registered and logged in with a username and password, can view images and messages posted to the group. In a closed group, messages and images are visible only to group members. .

16. The names and descriptions of all groups on "Hidden Service A" are listed and

visible to anyone who accesses the site, whether the group is open or closed. The number of members in any given group varies from a handful to dozens to hundreds to over a thousand. Although labeled as "Groups" on "Hidden Service A," the open groups which are accessible to all users essentially function as labels or subcategories for postings of distinct types of child pornography on the site. For example, the open group "Hardcore 2012 only," with 1146 members, states it is "for pictures and vids which are produced in 2012 only" and contains numerous images of infant and toddler aged children whose genitals are exposed and/or are being subjected to sexual abuse. The open group "Kindergarten Cuties (Girls 4-8)," which has 153 members, is described as "[a] group for lovers of cute and sexy girls between the ages of 4 to 8. NN, SC, or HC, as long as they're cute and young." In my training and experience, NN means non-nude, SC means softcore and refers to images that do not depict sex acts, and HC means hardcore and refers to images that depict sex acts. Images posted in that group are consistent with the group description. The group "Vicky's fans," with 428 members, states it is for "pedo's who like Vicky and the work she has done over the years." In my training and experience, "Vicky" is the name of a well-known and often traded series of child pornography involving the molestation of a prepubescent female by her father, who published the images to the Internet. That group contains images of that child pornography victim. The open group "Little Girl Anal Lovers," with 351 members, states it is for "those of us who have an [sic] strong . . . interest in the backdoor of little girls." The group page contains numerous images of infant and toddler aged children being sodomized. Other open groups with significant numbers of members are described below. The number of members as of November 17, 2012, are in parentheses, additional information as necessary is in parentheticals:

- Girl Penetration Lovers (981);

- Incest (713);
- Pedo women (637);
- Boy Pedo (574);
- Pedo-CinemaXXX* PEDOVIDS with NO LIMITS! (561)(in my training and experience, "no limits" refers to particularly violent hardcore sexual activity);
- Boys Hardcore (281);
- Young Girls Doublefucked (274);
- sperm boys and girls (266);
- Mother Daughter (261);
- Kindergarten (261);
- YoungBoysGettingFucked (251);
- BDSM (241)(in my training and experience, BDSM stands for bondage dominance sado-masochism);
- Baby lovers (236);
- Dads of girls (225);
- real rape vids (219).

Within those groups, the group descriptions and images posted within them are consistent with their group titles. All of those groups contain images of minor children engaging in sexually explicit conduct with adults or other children, or posed to expose their genitals. Postings of images of child pornography in many of the open groups have been made as recently as the last 24 hours, and in most if not all open groups within the past 30 days.

17. Images posted in closed groups are only accessible to members of those groups.

Examples of closed groups with significant numbers of members are described below. The number of members as of November 17, 2012, is in parentheses. Descriptions posted on the group page are in quotes and additional pertinent information is in parentheticals:

- Salty Milk (679)(described as "cumshots," i.e., images depicting children with semen on them);
- Kids with dogs and other animals (363);
- little sexy fuck girls (192) "discussion / pics for little girlies who youd like to fuck, stroke and wank over;"
- Toddler Girls Forced (152) "Girls Only!!! This group is for toddlers being penetrated, forced, bondage, and hurtcore. Will accept babies, toddlers, and a little older... if they are old enough for school.. they don't belong here! . . . Also, if you produce your own stuff and wish to share in a more closed setting... message me as I'm working on setting up a toddler private production site for both sharing among other producers and for private swapping.;"
- Fans of Tara (147)(in my training and experience, Tara is a reference to a known series of child pornography images;
- blowjobs (138) "nothing better than a preteen blow on my cock; "
- GooGoo's Place (120) "SERIOUS PEDO LOVERS ONLY" (group page includes a picture of an infant child being sodomized by an adult male penis);
- Boycam (58) "Here you will find boy captures from Omegle, Chatroulet, etc." (in my training and experience, Omegle and Chatroulette are webcam sites where a user can broadcast an image of him/herself online);

- Real Baby Lovers (0-1yo) "This group is for true Baby lusting pedos, who just get sooo hot and horny for little babies not even a year old;"
- Baby and Toddler Girl Lovers (0-5) Privet [sic] Group Only (39);
- Want to be my Partner? (37) "If being a partner in a CP business is something you'd like to do and you have money to help make it happen then private message me here or email at excitedgirl@tormail.org and we can go to the next step. As of right now I have 3 girls and plan to have another 3 when I have a suitable partner;"
- Boy Babysitters (36) "This is a group for those of us who babysit boys and want to share experiences or ideas;"
- Finding Them (22) "This is group where we discuss our techniques. Stories and Pics;"
- Siberian Mouse (13) (in my training and experience, Siberian Mouse in a known series of child pornography);
- Vintage Boys (8) "Cum inside and browse beautiful boys from bygone days;"

18. As reflected in two postings quoted in paragraph 17, "Hidden Service A" members utilize private messaging to communicate. Each of those quoted messages in paragraph 17 which reference private messaging were posted within the past 45 days. In addition, within the past 21 days, a "Hidden Service A" user posted following message [grammar and spelling errors in original]: "had a nice orgy with my nieces and some cousins. heres a pic from that night. message me if you hav any original material and want to private trade;"

19. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to

determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address was assigned at a given date and time. However, in the case of "Hidden Service A," the logs of member activity contain only the IP addresses of Tor "exit nodes" utilized by board users. A Tor "exit node" is the last computer through which the communications of a Tor user were routed before the communications reached their destination. It is not possible to trace such communications back through the Tor network to the actual user who sent the communications. Accordingly, those IP address logs cannot be used to locate and identify the users of "Hidden Service A."

E. THE NETWORK INVESTIGATIVE TECHNIQUE

20. Based on my training and experience as a Special Agent, as well as the experience of other law enforcement officers and computer forensic professionals involved in this investigation, and based upon all of the facts set forth herein, it is my belief that the network investigative technique applied for herein is the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity of those users of "Hidden Service A" described in Attachment A who are engaging in the federal offenses enumerated in paragraph 4. Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," as described herein, other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

21. Based on my training, experience, and the investigation described above, I have concluded that using a network investigative technique may help FBI agents locate the users of the

child pornography bulletin board "Hidden Service A." Accordingly, I request authority to use the NIT to investigate: (1) any user who accesses any page in the "Groups" or "Files" sections of "Hidden Service A" and (2) any user who sends or views a private message on "Hidden Service A" during the period of this authorization. In the normal course of operation, web sites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the web site would augment that content with some additional computer instructions. When a computer successfully downloads those instructions, the instructions are designed to cause the "activating" computer to deliver certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of that computer.

22. The NIT will reveal to the government environmental variables and certain registry-type information that may assist in identifying the computer, its location, and the user of the computer, as to which there is probable cause to believe they are evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B), Knowing Access or Attempted Access With Intent to View Child Pornography. In particular, the NIT will reveal to the government no information other than the following items, which are also described in Attachment B:

- The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
- In the ordinary course of business, "Hidden Service A" sends a unique session identifier to the activating computer to distinguish the data from that of other "activating" computers. This unique session identifier will be collected by the NIT;
- The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86).

23. Each of these categories of information described in Attachment B may constitute evidence of the crimes under investigation, including information that may help to identify the "activating" computer and its user. The actual IP address of a computer that accesses "Hidden Service A" can be associated with an Internet service provider ("ISP") and a particular ISP customer. The session identifier will distinguish the data from that of other "activating" computers. The type of operating system running on the computer can help to distinguish the user's computer from other computers located at the user's premises.

24. Based on my training, experience, and the investigation described herein, I know that network-level messages and information gathered directly from a sending computer can be more effective than other types of information in identifying a computer, its location and individual(s) using a computer. For instance, as described above, individual(s) using the Tor network can conceal their true originating IP address and thereby intentionally inhibit their identification. Getting IP address and other information directly from the computer being used by the subject can defeat such techniques.

25. During the thirty day period that the NIT is deployed on "Hidden Service A," each time that any user accesses any page in the "Groups" or "Files" sections of "Hidden Service A" or any user sends or views a private message on "Hidden Service A," the NIT authorized by this warrant will attempt to cause the user's computer to send the above-described information to a computer controlled by or known to the government.

F. REQUEST FOR DELAYED NOTICE

26. Rule 41(f)(3) allows for the delay of any notice required by the rule if authorized by statute. 18 U.S.C. § 3103a(b)(1) and (3) allows for any notice to be delayed if "the Court finds reasonable grounds to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in 18 U.S.C. § 2705) . . . ," or where the warrant "provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." Because there are legitimate law enforcement interests that justify the unannounced use of a NIT, I ask this Court to authorize the proposed use of the NIT without the prior announcement of its use. Announcing the use of the NIT could cause the members of "Hidden Service A" to undertake other measures to conceal their identity, or abandon the use of "Hidden Service A" completely, thereby defeating the purpose of the search.

27. The government submits that notice of the use of the NIT, as otherwise required by Federal Rule of Criminal Procedure 41(f), would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing "Hidden Service A." It would, therefore, seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence

of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).

28. Furthermore, the investigation has not yet identified an appropriate person to whom such notice can be given. Thus, the government requests authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing "Hidden Service A" has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

29. The government further submits that, to the extent that use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no way to view the information and to use it to further the investigation. Furthermore, the NIT does not deny the users access to "Hidden Service A" or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

G. TIMING OF SEIZURE/REVIEW OF INFORMATION

30. Rule 41(e)(2) requires that the warrant command FBI "to execute the warrant within a specified period of time no longer than fourteen days" and to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." After the server hosting "Hidden Service A" is seized, it will remain in law enforcement custody. Accordingly, the government requests authority to employ the NIT onto "Hidden Service A" at any time of day, within fourteen days of the Court's authorization. The NIT will be used on "Hidden Service A" for not more than 30-days from the date of the issuance of the warrant.

31. For the reasons above and further, because users of "Hidden Service A" communicate on the board at various hours of the day, including outside the time period between 6:00 a.m. and 10:00 p.m., and because the timing of the user's communication on the board is solely determined by when the user chooses to access the board, rather than by law enforcement, I request authority for the NIT to be employed at any time a user's computer accesses the board, even if that occurs outside the hours of 6:00 a.m. and 10:00 p.m. Further, I seek permission to review information transmitted to a computer controlled by or known to the government, as a result of the NIT, at whatever time of day or night the information is received.

32. The government does not currently know the exact configuration of the computers that may be used to access "Hidden Service A." Variations in configuration, e.g., different operating systems, may require the government to send more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the activating computers for up to 30 days after this warrant is authorized.

33. The Government may, if necessary, seek further authorization from the Court to employ the NIT on "Hidden Service A" beyond the 30-day period authorized by this warrant.

H. SEARCH AUTHORIZATION REQUESTS

34. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

a. the NIT may cause an activating computer – wherever located – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location,

other information about the computer and the user of the computer, as described above and in Attachment B;

b. the use of multiple communications, without prior announcement, within 30 days from the date this Court issues the requested warrant;

c. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by or known to the government;

d. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an "activating" computer that accessed "Hidden Service A" has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

I. REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

35. I further request that this application and the related documents be filed under seal. This information to be obtained is relevant to an ongoing investigation. Premature disclosures of this application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.

J. CONCLUSION

36. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access "Hidden Service A," in violation of 18 U.S C. §§ 2251 and 2252A.

37. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

38. Based on the information described above, there is probable cause to believe that employing a NIT on "Hidden Service A," to collect information described in Attachment B, will result in the FBI obtaining the evidence and instrumentalities of the child exploitation crimes described above.

Sworn to under the pains and penalties of perjury.

Jeffrey Tarpinian

Jeffrey Tarpinian

Special Agent

Sworn to and subscribed before me this 17th day of November, 2012

United States Magistrate Judge

ATTACHMENT A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography bulletin board "Hidden Service A," identified by its Tor URL of "oqm66m6iyt6vxk7k.onion," which is located on a computer server at a government facility in the District of Nebraska.

The activating computers are those of: (1) any user who accesses any page in the "Groups" or "Files" sections of "Hidden Service A" and (2) any user who sends or views a private message on "Hidden Service A" during the period of this authorization.

The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

- The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
- A unique session identifier sent by "Hidden Service A;"
- The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86).

to the extent such information is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B), Knowing Access or Attempted Access With Intent to View Child Pornography.